СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	–	База данных
ЭВТ	–	Электронная вычислительная техника
ЭП	–	Квалифицированная электронная подпись/усовершенствованная электронная подпись
ИТС	–	Информационно-телекоммуникационная система
КЗЗ	–	Комплекс средств защиты
КСЗИ	–	Комплексная система защиты информации
КТЗ	–	Комплекс технических средств
ЛОМ	–	Локальная вычислительная сеть
МЕ	–	Межсетевой экран
МКМ	–	Сетевой криптомодуль
НКИ	–	Носитель ключевой информации
НСД	–	Несанкционированный доступ
ПО	–	Программное средство
РС	–	Рабочая станция
ТС	–	Техническое задание
ЦЗО	–	Центральный удостоверяющий орган
Придавец	–	Квалифицированный поставщик электронных доверительных услуг
CMP	–	Certificate management protocol (протокол управления сертификатами)
HTTP	–	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	–	HyperText Transfer Protocol Secure (безопасный протокол передачи данных)
IPS	–	Intrusion prevention system (система предупреждения вторжений)
OCSP	–	Online Certificate Status Protocol (протокол определения статуса сертификата)
PKCS	–	Public Key Cryptography Standarts (стандарты криптографии с открытым ключом)
RDP	–	Remote Desktop (удаленный рабочий стол)
SQL	–	Structured Query Language (язык структурированных запросов)
SSH	–	Secure Shell (безопасная оболочка)
TCP	–	Transmission Control Protocol (протокол управления передачей)
TSP	–	TimeStamp Protocol (протокол формирования метки времени)
VPN	–	Virtual Private Network (виртуальная частная сеть)

1 ОБЩЕЕ ОПИСАНИЕ

Интегрированная система электронной идентификации (ИСЕИ, id.gov.ua) – универсальная платформа предназначена для:

- электронной идентификации и аутентификации пользователей с помощью электронных подписей (на файловом, облачном или других защищенных носителях), Действие.Подпись, Действие.OAuth и BankID НБУ**(сервис аутентификации пользователей)**;

- наложение и проверка электронной подписи через веб**(виджет подписи)**.

Владельцем системы государство в лице Министерства цифровой трансформации Украины. Обладателем информации, обрабатываемой в ИСЕИ, является держатель системы.

Администратором и техническим администратором ИСЕИ является государственное предприятие «ДЕЯ». Субъектами взаимодействия являются:

- органы государственной власти, органы местного самоуправления, их должностные лица;

- юридические лица и физические лица – предприниматели;

- поставщики электронных доверительных услуг и поставщики услуг электронной идентификации;

- администраторы промежуточных узлов электронной идентификации (хабов);

- администратор;

- держатель системы.

Объектами взаимодействия являются:

- средства электронной идентификации в контексте используемых схем электронной идентификации пользователи системы для осуществления процедур электронной идентификации;

– информационно-коммуникационные системы органов государственной власти, органов местного самоуправления;

- информационно-коммуникационные системы юридических лиц и физических лиц – предпринимателей;

- информационно-коммуникационные системы, реализующие схемы электронной идентификации;

- информационно-коммуникационные системы, реализующие схемы электронной идентификации в рамках трансграничной электронной идентификации

Система работает круглосуточно семь дней в неделю.

Доступ к системе осуществляется через открытый информационный ресурс, имеющий официальный адрес в Интернете – https://id.gov.ua.

2 ПОРЯДОК ОБРАБОТКИ ИНФОРМАЦИИ

2.1 Общая характеристика сервиса аутентификации

Подключение к сервису проверки подлинности пользователей Системы осуществляется с целью электронной идентификации и аутентификации пользователей через схемы идентификации (электронная подпись, Действие. Подпись, Действие. OAuth, BankID).

Система при функционировании взаимодействует с серверами прикладных систем, пользователями (клиентами) прикладных систем, со схемами электронной идентификации Установщиков, схемами электронной идентификации других поставщиков услуг по электронной идентификации, в том числе с серверами банковской идентификации, подключенных к промежуточному узлу электронной и Банк ID НБУ.

Схемы электронной идентификации Наставников, схемы электронной идентификации других поставщиков услуг по электронной идентификации, в том числе серверы банковской идентификации, подключенные к промежуточному узлу электронной идентификации (хабу) Банк ID НБУ, должны соответствовать требованиям законодательства по защите информации и иметь разрешительные документы защиты информации, в том числе, отвечать Требованиям к средствам электронной идентификации, уровням доверия к средствам электронной идентификации для их использования в сфере электронного управления, утвержденных приказом Министерства цифровой трансформации Украины от 05.12.2022 № 130.

Порядок взаимодействия составных частей ИСЭИ при идентификации пользователя (клиента) на сервере прикладной системы реализуется в соответствии с протоколом**OAuth 2.0.**

Для идентификации серверов прикладных систем на сервере идентификации ИСЭИ соответствующие прикладные системы предварительно регистрируются на сервере идентификации и согласно протоколу OAuth для каждой прикладной системы устанавливаются следующие параметры:

– идентификатор прикладной системы**client_id**, однозначно идентифицирующий прикладную систему (значение идентификатора приведено для тестовой прикладной системы зарегистрированной на тестовом сервере идентификации);

– секретная строчка доступа**client_secret**, по которой сервер идентификации будет выдавать серверу прикладной системы маркер доступа -**access_token**;

– сертификат открытого ключа протокола распределения ключей прикладной системы, назначенный для направленного шифрования полученной информации о пользователе (клиенте) при передаче между сервером идентификации ИСЭИ и сервером прикладной системы.

2.2 Порядок электронной идентификации по электронной подписи, Действие.

Порядок взаимодействия составных частей ИСЭИ при идентификации пользователя (клиента) Системы на сервере прикладной системы должны включать:

1)отправку пользователем (клиентом) запроса на идентификацию с web-браузера на web-странице webсервера прикладной системы (нажатие ссылки или контекстная отправка запроса) по методу GET протокола HTTP(S);

2) обработку запроса и отправку web-сервером прикладной системы пользователю ответа с перенаправлением браузера пользователя на соответствующую страницу сервера идентификации (перенаправленная ссылка);

3) отправку пользователем запроса на отображение соответствующей страницы сервера идентификации по методу GET протокола HTTPS на перенаправленную ссылку вида:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=dig_sign,diia_id&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметры запроса описаны в табл. 2.2.1. Входящие параметры проверяются в соответствии с приложением А.

Таблица 2.2.1 – Описание параметров запроса пользователя сервера идентификации

Параметры	Описание
response_type	Должен иметь значение**code**
client_id	Идентификатор прикладной системы (приведенное значение для примера)
auth_type	Параметр, определяющий возможные средства идентификации (задается перечень необходимых средств аутентификации, приведенное значение для примера)
state	Параметр, значение которого должно быть возвращено при переадресации на адрес, указанный в значении**redirect_uri**(значение приведено в качестве примера). Значение должно быть случайным.
redirect_uri	Обратная ссылка (URI) на web-сервер прикладной системы (значение ссылки **http(s)://url/redirect**приведено для примера), на которое сервер идентификации перенаправит пользовательский браузер после выполнения процедуры идентификации

Обратная ссылка (**redirect_uri**) также может быть предварительно установлено на сервере идентификации вместе с идентификатором прикладной системы (**client_id)**и секретной строчкой доступа (**client_secret)**у регистрационных данных соответствующей прикладной системы. В этом случае сервер прикладной системы может не передавать обратную ссылку в запросе, а сервер идентификации будет брать его из регистрационных данных прикладной системы;

4) обработку запроса и отправку сервером идентификации пользователю ответа с содержимым webстраницы идентификации и библиотеками подписи пользователя Надавателя (загрузка java-скрипта браузером или подключение предварительно установленных web-библиотек подписи пользователя Надавателя);

5) считывание пользователем собственного личного ключа с использованием соответствующей библиотеки подписи;

6) формирование пользователем ЭП – подпись данных идентификации с использованием соответствующей библиотеки подписи;

7) отправку пользователем запроса на идентификацию с подписанным данным сервера идентификации по методу POST протокола HTTPS;

8) проверку сервером идентификации ИСЭИ подписанных данных идентификации от пользователя с использованием библиотеки подписи в виде модуля расширения PHP и сетевого криптомодуля и принятия решения об успешности идентификации пользователя;

9) отправку (в случае успешной идентификации) сервером идентификации пользователю ответа с перенаправлением браузера пользователя на страницу сервера прикладной системы, указанной в качестве обратной ссылки (**redirect_uri**) при предварительном перенаправлении на сервер идентификации;

10) отправку пользователем (по результату перенаправления браузера) запроса на завершение идентификации сервера прикладной системы по методу GET протокола HTTP(S) на перенаправленную ссылку вида:

```
GET

http(s)://url/redirect?code=code&
    state=state
```

Параметры запроса описаны в табл. 2.2.2.

Таблица 2.2.2 – Описание параметров запроса пользователя на завершение идентификации

Параметры	Описание
http(s)://url/redirect	Обратная ссылка на страницу web-сервера прикладной системы (**redirect_uri**)
code	Код авторизации
state	Значение, отправленное в запросе на шаге 3

11)обработку сервером прикладной системы запроса на завершение идентификации пользователя, включающей:

11.1) отправку сервером прикладной системы запроса сервера идентификации на получение маркера доступа по коду завершения идентификации (**code**) методом GET или POST протокола HTTPS вида:

```
GET/POST

https://id.gov.ua/get-access-token?grant_type=authorization_code&
    client_id= client_id &
    client_secret= client_secret &
    code=code
```

Примечание.Код авторизации (**code**) может быть использован только один раз.

11.2) обработку запроса и отправку сервером идентификации сервера прикладной системы ответа с маркером доступа в виде JSON-текста вида:

```
Content-Type: application/json {


    «access_token»:«»,
    "token_type":"bearer",
    "expires_in":"",
    "refresh_token":"",
    «user_id»:«»
}
```

Параметры ответа описаны в табл. 2.2.3.

Таблица 2.2.3 – Описание параметров ответа сервера прикладной системы с маркером доступа

Параметры	Описание
access_token	Маркер доступа (значение маркера приведено в качестве примера)
token_type	Тип маркера доступа (имеет фиксированное значение для применения средствами идентификации –**bearer**– доступ по маркеру для предъявителя)

expires_in	Время завершения действия маркера доступа
user_id	Идентификатор идентифицированного пользователя, по которому может быть получена информация о пользователе
refresh_token	Маркер для получения нового маркера доступа

Примечание.Маркер доступа (**access_token**) может быть использован только один раз. Для повторного обращения следует использовать**refresh_token**.

В сервере идентификации идентификаторы идентифицированных пользователей (**user_id**) хранятся вместе с информацией из сертификатов пользователей во временной базе данных (БД) и время завершения действия маркера доступа (**expires_in**) указывает на срок существования соответствующих записей в БД. В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.2.4.

Таблица 2.2.4 – Описание параметров ошибки ответа сервера прикладной системы с маркером доступа

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

11.3) отправка сервером прикладной системы следующего запроса к серверу идентификации на получение информации о пользователе по маркеру доступа (**access_token**) методом GET или POST протокола HTTPS вида:

```
GET/POST

https://id.gov.ua/get-user-info?&access_token=access_token&
    user_id=36&
    fields=issuer,issuercn,serial,subject,subjectcn,locality,state,o,ou,title,lastname,
    middlename,givenname,email,address,phone,dns,edrpoucode,drfocode&
    cert=
```

Параметры запроса описаны в табл. 2.2.5.

Таблица 2.2.5 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
access_token	Маркер доступа
user_id	Идентификатор идентифицированного пользователя (приведенное значение для примера)
fields	Названия полей сертификата запрашиваемых пользователей. Если названия полей (**fields**) не указаны, то возвращаются все доступные поля сертификата с информацией о пользователе (владельце сертификата) и издателе (Предоставитель)
cert	Сертификат шифрования (протокола распределения ключей), на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными поставщиками доверительных услуг, перечень которых доступен на сайте ЦЗО

	https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.

11.4) обработка сервером идентификации запроса путем формирования зашифрованного (с использованием библиотеки подписи в виде модуля расширения PHP и сетевого криптомодуля) ответа с информацией об идентифицированном пользователе в виде JSON-текста вида:

```
Content-Type: application/json {

    "auth_type":"dig_sign",
    "issuer":"",
    "issuercn":"",
    "serial":"",
    «subject»:«»,
    «subjectcn»:«»,
    «locality»:«»,
    «state»:«»,
    «o»:«»,
    "ou":"",
    «title»:«»,
    "lastname":"",
    "givenname":"",
    "middlename":"",
    «email»:«»,
    "address":"",
    "phone":"",
    dns:
    edrpoucode:
     «unzr»:«»,
    «drfocode»:«»
}
```

Все возможные поля сертификата пользователя, возвращаемые сервером идентификации после идентификации пользователя (клиента) системы через Податчика (по ЭП), приведены в табл. 2.2.6.

Таблица 2.2.6

Название поля (одно из значений названий полей **fields**)	Описание содержимого поля
issuer	Реквизиты издателя сертификата.
issuercn	Общее имя Податчика
serial	Регистрационный номер сертификата в Надавателе
subject	Реквизиты владельца сертификата (пользователя)
subjectcn	Общее имя пользователя
locality	Город (населенный пункт) пользователя
state	Область (регион) пользователя
o	Наименование пользовательской организации
ou	Название подразделения организации пользователя
title	Должность пользователя
givenname	Имя пользователя
middlename	Отчество пользователя
lastname	Фамилия пользователя
email	Адрес эл. почты (e-mail) пользователя
address	Адрес (физический) пользователя
phone	Телефон пользователя
dns	DNS-имя пользователя
edrpoucode	Код по ЕГРПОУ пользователя

drfocode	РНОКПП пользователя или серия (при наличии) и номер паспорта (для пользователей,которые по своим религиозным убеждениям отказываются от принятие регистрационного номера учетной карточки налогоплательщика и официально уведомили об этом соответствующий контролирующий орган и имеют отметку в паспорте) (Приложение А, п. 8)
unzr	Уникальный номер записи в Едином демографическом реестре

Все возможные поля сертификата пользователя, возвращаемые сервером идентификации после идентификации пользователя (клиента) системы через Податчика за Действие. Подпись приведена в табл.

Таблица 2.2.7

Название поля (одно из значений названий полей fields)	Описание содержимого поля
issuer	Реквизиты издателя сертификата.
issuercn	Общее имя Податчика
serial	Регистрационный номер сертификата в Надавателе
subject	Реквизиты владельца сертификата (пользователя)
subjectcn	Общее имя пользователя
givenname	Имя пользователя
middlename	Отчество пользователя
lastname	Фамилия пользователя
drfocode	РНОКПП пользователя или серия (при наличии) и номер паспорта (для пользователей, которые по своим религиозным убеждениям отказываются от принятия регистрационного номера учетной карточки налогоплательщика и официально сообщили об этом соответствующий контролирующий орган и имеют отметку в паспорте) (Приложение А, п. 8)
unzr	Уникальный номер записи в Едином демографическом реестре

Параметры ответа описаны в табл. 2.2.7.

Таблица 2.2.7 – Описание параметров ответа с информацией об идентифицированном пользователе

Параметры	Описание
auth_type	Тип аутентификации, выбранный пользователем (возможные варианты: **dig_sign**,**diia_id**)
issuer,**issuercn**и др.	Соответствующие поля пользовательского сертификата (значения полей приведены для примера)

Ответ отправляется в виде JSON-текста вида:

```
Content-Type: application/json {

    "encryptedUserInfo":""
}
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.2.8.

Таблица 2.2.8 – Описание параметров ошибки ответа с информацией об идентифицированном пользователе

Параметры	Описание

error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

11.5) отправку сервером идентификации сервера прикладной системы зашифрованной ответы с информацией об идентифицированном пользователе;

11.6) получение и расшифрование сервером прикладной системы ответа с информацией о пользователе (клиенте) и принятие решения сервером прикладной системы о завершении идентификации;

12) отправку сервером прикладной системы ответа пользователю о завершении идентификации.

2.3 Порядок электронной идентификации банковских учреждений (BankID)

Порядок взаимодействия составных частей системы при идентификации пользователя (клиента) системы на сервере прикладной системы с использованием банковских учреждений (BankID) должен включать:

1) отправку пользователем (клиентом) запроса на идентификацию с web-браузера на web-странице web-сервера прикладной системы (нажатие ссылки или контекстная отправка запроса) по методу GET протокола HTTP(S);
2) обработку запроса и отправку web-сервером прикладной системы пользователю ответа с перенаправлением браузера пользователя на соответствующую страницу сервера идентификации (перенаправленная ссылка);
3) отправку пользователем запроса на отображение соответствующей страницы сервера идентификации по методу GET протокола HTTPS на перенаправленную ссылку вида:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=bank_id&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметры запроса описаны в табл. 2.3.1. Входные параметры проверяются в соответствии с приложением А. Таблица

2.3.1 – Описание параметров пользовательского запроса сервера идентификации

Параметры	Описание
response_type	Должен иметь значение**code**
client_id	Идентификатор прикладной системы (приведенное значение для примера)
auth_type	Параметр, определяющий возможные средства идентификации (задается перечень необходимых средств аутентификации, приведенное значение для примера)
state	Параметр, значение которого должно быть возвращено при переадресации на адрес, указанный в значении**redirect_uri**(значение приведено в качестве примера). Значение должно быть случайным.
redirect_uri	Обратная ссылка (URI) на web-сервер прикладной системы (значение ссылки **http(s)://url/redirect**приведено для примера), на которое сервер идентификации перенаправит пользовательский браузер после выполнения процедуры идентификации

Обратная ссылка (**redirect_uri**) также может быть предварительно установлено на сервере идентификации вместе с идентификатором прикладной системы (**client_id)**и секретной строчкой доступа (**client_secret)**у регистрационных данных соответствующей прикладной системы. В этом случае сервер прикладной системы может не передавать обратную ссылку в запросе, а сервер идентификации будет брать его из регистрационных данных прикладной системы;

4) обработку запроса и отправку сервером идентификации пользователю ответа с содержанием веб-страницы идентификации;
5) отправку пользователем запроса на банковскую идентификацию по методу GET протокола HTTPS;

6) отправку пользователем запроса на отображение соответствующей страницы сервера банковской идентификации по методу GET протокола HTTPS на перенаправленную ссылку вида:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    redirect_uri=http(s)://url/redirect&
    state=
```

Параметры запроса описаны в табл. 2.3.2.

Таблица 2.3.2 – Описание параметров запроса пользователя на сервер банковской идентификации

Параметры	Описание
client_id	Идентификатор прикладной системы
redirect_uri	Обратная ссылка (URI) на web-сервер идентификации (значение ссылки **http(s)://url/redirect**(приведенное для примера), на которое сервер банковской идентификации перенаправит браузер пользователя после выполнения процедуры идентификации
state	Параметр, значение которого должно быть возвращено сервером банковской идентификации при переадресации на адрес сервера идентификации, указанный в значении**callback_url**. Используется во избежание CSRF атак

7) запрос на отображение формы идентификации сервером банковской идентификации (по результату переадресации);
8) формирование формы идентификации сервером банковской идентификации и отправка пользователю;
9) заполнение и отправка пользователем формы идентификации на web-странице сервера банковской идентификации;
10) обработку запроса и отправку сервером банковской идентификации пользователю ответа с перенаправлением браузера пользователя на соответствующую страницу сервера идентификации (перенаправленная ссылка);
11) отправку пользователем запроса на отображение соответствующей страницы сервера идентификации по методу GET протокола HTTPS на перенаправленную ссылку вида:

```
GET

http(s)://url/redirect?code=code&
    state=state
```

Параметры запроса описаны в табл. 2.4.3.

Таблица 2.3.3 – Описание параметров пользовательского запроса на сервер идентификации

Параметры	Описание
http(s)://url/redirect	Обратная ссылка на страницу web-сервера идентификации (**redirect_uri**)
code	Код авторизации (authorization code)
state	Значение, которое использовалось при ответе с кодом авторизации

Если при запросе возникали ошибки, то:

- или сервер банковской идентификации не удалось идентифицировать на сервере банка (в частности, не зарегистрирован на стороне банка, не совпадает значение параметра**client_id**) или некорректный запрос. В таком случае описание ошибки будет отображено на web-странице сервера банка;
- или пользователя удалось идентифицировать на ресурсе сервера банка, однако произошло другое ошибка – будет выполнена переадресация в адрес параметра**redirect_uri**с последующими параметрами в теле запроса (body) в формате JSON.

В случае ошибки в случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error": "invalid_grant",
    "error_description": "",
    "state": ""
}
```

Параметры ответа описаны в табл. 2.3.4.

Таблица 2.3.4 – Описание параметров ответа при возникновении ошибки

Параметры	Описание
error	Один из определенных кодов ошибки согласно протоколу OAuth. В частности: **invalid_request, unauthorized_client**, **access_denied, unsupported_response_type, invalid_scope, server_error, temporarily_unavailable**
error_description	Возможное текстовое описание ошибки, детализация для разработчиков
state	Значение, которое использовалось при ответе с кодом авторизации

12) обмен данными с сервером банковской идентификации:

12.1) отправку сервером идентификации запроса серверу банковской идентификации на получение маркера доступа (**access_token**). Запрос методом POST вида:

```
POST

https://url/token

HTTP/1.1

Content-Type: application/x-www-form-urlencoded

    grant_type=authorization_code&
    client_id=client_id&
    client_secret=client_secret&
    code=code&
    redirect_uri=callback_url
```

Параметры запроса описаны в табл. 2.4.5.

Таблица 2.3.5 – Описание параметров запроса на получение маркера доступа к серверу идентификации

Параметры	Описание
grant_type	Тип запроса, который должен иметь значение**authorization_code**». (В противном случае, запрос на продление действия маркера доступа (**access_token**), значение будет «**refresh_token**»)
code	Код авторизации (**authorization code**), полученный на предыдущем шаге
callback_url	Адрес сервера идентификации, в данном случае используется для переадресации при возникновении ошибок при получении маркера доступа (**access_token**)

12.2) ответ сервера банковской идентификации с маркером доступа в виде JSONструктуры:

```
Content-Type: application/json {

    "token_type":"bearer",
    «access_token»:«»,
    "expires_in":"",
    "refresh_token":"
}
```

В случае возникновения ошибок обработки запроса, соответствующий сервер банка переадресовывает пользователя на адрес callback_url и указывает нижеуказанные параметры и значения, повлекшие отказ. Параметры со значениями передаются в теле запроса (body) в формате JSON. В случае ошибки в случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error": "invalid_grant",
    "error_description": "",
    "state": ""
}
```

Параметры ответа описаны в табл. 2.4.6.

Таблица 2.3.6 – Описание параметров ответа при возникновении ошибки

Параметры	Описание
error	Один из определенных кодов ошибки согласно протоколу OAuth. В частности: **invalid_request, unauthorized_client**, **access_denied, unsupported_response_type, invalid_scope, server_error, temporarily_unavailable**
error_description	Возможное текстовое описание ошибки, детализация для разработчиков
state	Значение, которое использовалось при ответе с кодом авторизации

12.3) запрос сервера идентификации данных пользователя. Предоставление запроса сертификата шифрования.

Предоставление данных происходит на основании маркера доступа (**access_token**), полученного в ходе авторизации (согласно предыдущему пункту). Маркер доступа передается в заголовке запроса (**headers**) в виде:

```
Authorization:«Bearer access_token»
```

Сервер идентификации в запросе к серверу банковской идентификации должен указать, какой именно набор данных по клиенту нужно передать в ответе, а также предоставить свой сертификат шифрования в формате base64. Сервер банковской идентификации запрашивает сервер банка, в котором в свою очередь указывает перечень необходимых данных и предоставляет сертификат шифрования сервера идентификации, для которого осуществляется аутентификация клиента. Сертификат шифрования передается в атрибуте. **cert**» в формате BASE64.

Перечень необходимых данных указывается согласно допустимым полям в виде JSON-объекта в теле запроса (**body**). Если какое-либо из полей отсутствует со стороны сервера идентификации, то заказанное поле возвращается пустым.

Пример JSON-объекта по запросу персональных данных:

```
{
    "type":"physical",
    «cert»:«»,
    «fields»:[
        firstName,
        middleName,
        "lastName",
        "phone",
        «inn»
    ]
}
```

12.4) обработка сервером банковской идентификации запроса путем формирования, подписи и зашифрования ответа с информацией об идентифицированном пользователе в виде JSON-текста вида:

```
{
   "state":"ok",
   «cert»:«»,
  customerCrypto:
}
```

содержащий JSON-объект**«customer»**с персональными данными пользователя в виде:

```
«customer»:{
   "type":"physical",
   "inn":"",
   «email»:«»,
   "firstName":"",
   "lastName":"",
   "middleName":"",
   "phone": ""
}
```

Значение**физический,**приведены в качестве примера.

Все возможные поля с информацией о пользователе, возвращаемые сервером идентификации после идентификации пользователя (клиента) системы через банковские учреждения (BankID) приведены в табл. 2.3.7.

Таблица 2.3.7 - Все возможные поля, возвращаемые сервером идентификации после идентификации через банковские учреждения (BankID).

Название структуры	Название поля (одно из значений названий полей структуры)	Описание содержимого поля
	state	
	cert	Сертификат шифрования (в формате BASE64) отправителя данных
	customerCrypto	Содержит зашифрованную структуру**customer** (зашифрованные данные в формате BASE64)
customer	**lastName**	Фамилия
	firstName	Имя
	middleName	Отчество
	phone	Телефон пользователя
	inn	РНОКПП пользователя или серия (при наличии) и номер паспорта (для пользователей,которые через свои религиозные убеждения отказываются от принятия регистрационного номера учетной карточки налогоплательщика и официально сообщили об этом соответствующему контролирующему органу и имеют отметку в паспорте (Приложение А, п. 8)
	email	Адрес эл. почты (e-mail)

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

   "error":"invalid_grant",
   "error_description":""
}
```

Параметры ответа описаны в табл. 2.3.8.

Таблица 2.3.8 – Описание параметров ошибки

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

12.5) отправка сервером идентификации запроса у Податчика на поиск и проверку статуса сертификата отправителя (сервера банковской идентификации) по протоколу OCSP и получения ответа и загрузки от Подавателя текущих CBC и/или проверку статуса сертификата с использованием загруженных ответных CBC/OCSP;

12.6) отправка запроса по расшифровке и проверке ЭП информации о пользователе сетевом криптомодуле и получении ответа по расшифрованной информации;

12.7) формирование сервером идентификации запроса на получение статуса сертификата сервера прикладной системы к Податчику и получение ответа;

13) отправку пользователю соответствующей страницы сервером идентификации путем перенаправления (протокол взаимодействия с пользователем HTTPS) для подтверждения данных.

14) отправку сервером идентификации запроса в завершение идентификации сервера прикладной системы по методу GET протокола HTTP(S) на перенаправленную ссылку вида:

GET

http(s)://url/redirect?code=code&
state=state

Параметры запроса описаны в табл. 2.3.5.

Таблица 2.3.5 – Описание параметров запроса сервера идентификации в завершение идентификации

Параметры	Описание
http(s)://url/redirect	Обратная ссылка на страницу web-сервера прикладной системы (**redirect_uri**)
code	Код авторизации
state	Значение, отправленное в запросе на шаге 3

15) обработку сервером прикладной системы запроса на завершение идентификации пользователя, включающего:

15.1) отправку сервером прикладной системы запроса серверу идентификации на получение маркера доступа по коду завершения идентификации (**code**) методом GET или POST протокола HTTPS вида:

GET/POST

https://id.gov.ua/get-access-token?grant_type=authorization_code&
client_id=client_id&
client_secret=client_secret&
code=code

Примечание.Код авторизации (**code**) может быть использован только один раз.

15.2)обработку запроса и отправку сервером идентификации сервера прикладной системы ответа с маркером доступа в виде JSON-текста вида:

Content-Type: application/json {

«access_token»:«»,
"token_type":"bearer",

```
    "expires_in":"",
    "refresh_token":"",
    «user_id»:«»
}
```

Параметры ответа описаны в табл. 2.3.9.

Таблица 2.3.9 – Описание параметров ответа сервера прикладной системы с маркером доступа

Параметры	Описание
access_token	Маркер доступа (значение маркера приведено в качестве примера)
token_type	Тип маркера доступа (имеет фиксированное значение для применения средствами идентификации –**bearer**– доступ по маркеру для предъявителя)
expires_in	Время завершения действия маркера доступа
user_id	Идентификатор идентифицированного пользователя, по которому может быть получена информация о пользователе
refresh_token	Маркер для получения нового маркера доступа

Примечание.Маркер доступа (**access_token**) может быть использован только один раз. Для повторного обращения следует использовать**refresh_token**.

В сервере идентификации идентификаторы идентифицированных пользователей (user_id) хранятся вместе с информацией из сертификатов пользователей во временной базе данных (БД) и время завершения действия маркера доступа (expires_in) указывает срок существования соответствующих записей в БД.

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {


    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.3.10.

Таблица 2.3.10 – Описание параметров ошибки ответа сервера прикладной системы

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

15.3) отправку сервером прикладной системы следующего запроса к серверу идентификации на получение информации о пользователе по маркеру доступа (**access_token**) и предоставление при запросе сертификата протокола распределения для направленного шифрования, методом GET или POST протокола HTTPS вида:

```
GET/POST

https://id.gov.ua/get-user-info?&access_token=&
    user_id=36&
    fields=issuer,issuercn,serial,subject,subjectcn,locality,
    state,o,ou,title,surname,givenname,email,address,phone,dns,edrpoucode,drfocode,documents&
    cert=
```

Предоставление данных производится на основании маркера доступа (access_token), полученного в ходе авторизации (согласно предыдущему пункту). Маркер доступа передается в заголовке запроса (headers) в виде:

```
Authorization:«Bearer access_token»
```

Параметры запроса описаны в табл. 2.3.11.

Таблица 2.3.11 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
access_token	Маркер доступа
user_id	Идентификатор идентифицированного пользователя (приведенное значение для примера)
fields	Названия полей с информацией о запрашиваемых пользователях. Если названия полей (fields) не указаны, возвращаются все доступные поля с информацией о пользователях, поступающих от системы BankID.
cert	Сертификат шифрования (протокола распределения ключей), на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными поставщиками доверительных услуг, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.

15.4) формирование запроса на получение отметки времени к Податчику и получение ответа с меткой времени.

15.5)обработка сервером идентификации запроса путем формирования, подписи и зашифрования (с использованием библиотеки подписи в виде модуля расширения PHP и сетевого криптомодуля) ответа с информацией об идентифицированном пользователе в виде JSON-текста вида:

```
Content-Type: application/json {

    "auth_type":"bank_id",
    "lastname":"",
    "givenname":"",
    "middlename":"",
    «email»:«»,
    "phone":"",
    «drfocode»:«»
}
```

Параметры ответа описаны в табл. 2.3.12.

Таблица 2.3.12 – Описание параметров ответа с информацией об идентифицированном пользователе

Параметры	Описание
auth_type	Тип аутентификации, выбранный пользователем (возможные варианты: **bank_id**)
issuer,**issuercn**и др.	Соответствующие поля данных пользователя (значения полей приведены для примера)

Все данные об адресе вносятся в одно поле**address.**

Ответ отправляется в виде JSON-текста вида:

```
Content-Type: application/json {

    "encryptedUserInfo":""
}
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.4.13.

Таблица 2.3.13 – Описание параметров ошибки ответа с информацией об идентифицированном пользователе

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

15.6) отправку сервером идентификации сервера прикладной системы зашифрованного и подписанного ответа с информацией об идентифицированном пользователе;

15.7) получение, расшифровка и проверка ЭП сервером прикладной системы ответа с информацией о пользователе (клиенте) и принятие решения сервером прикладной системы о завершении идентификации;

16) отправку сервером прикладной системы ответа пользователю о завершении идентификации.

2.4 Порядок электронной идентификации по Действу. OAuth

Порядок взаимодействия составных частей ИСЭИ при идентификации пользователя (клиента) ИСЭИ на сервере прикладной системы через Действие. OAuth должен включать:

1)отправку пользователем (клиентом) запроса на идентификацию с web-браузера на web-странице webсервера прикладной системы (нажатие ссылки или контекстная отправка запроса) по методу GET протокола HTTP(S);

2) обработку запроса и отправку web-сервером прикладной системы пользователю ответа с перенаправлением браузера пользователя на соответствующую страницу сервера идентификации (перенаправленная ссылка);

3) отправку пользователем запроса на отображение соответствующей страницы сервера идентификации по методу GET протокола HTTPS на перенаправленную ссылку вида:

```
GET

https://id.gov.ua/?response_type=code&
    client_id=client_id&
    auth_type=diia_oauth&
    state=state&
    redirect_uri= http(s)://url/redirect
```

Параметры запроса описаны в табл. 2.4.1. Входящие параметры проверяются в соответствии с приложением А.

Таблица 2.4.1 – Описание параметров запроса пользователя сервера идентификации

Параметры	Описание
response_type	Должен иметь значение**code**
client_id	Идентификатор прикладной системы (приведенное значение для примера)
auth_type	Параметр, определяющий возможные средства идентификации (задается перечень необходимых средств аутентификации, приведенное значение для примера)
state	Параметр, значение которого должно быть возвращено при переадресации на адрес, указанный в значении**redirect_uri**(значение приведено в качестве примера). Значение должно быть случайным.

redirect_uri	Обратная ссылка (URI) на web-сервер прикладной системы (значение ссылки **http(s)://url/redirect**приведено для примера), на которое сервер идентификации перенаправит пользовательский браузер после выполнения процедуры идентификации

4) обработку запроса и отправку сервером идентификации пользователю ответа с содержанием веб-страницы идентификации;

5) отправку пользователем запроса на идентификацию через Действие OAuth по методу GET протокола HTTPS;

6) считывание пользователем QR-код сканером в приложении «Действие» и подтверждение идентификации в приложении «Действие»;

7) отправку пользователем (по результату перенаправления браузера) запроса на завершение идентификации сервера прикладной системы по методу GET протокола HTTP(S) на перенаправленную ссылку вида:

GET

http(s)://url/redirect?code=code&
state=state

Параметры запроса описаны в табл. 2.4.2.

Таблица 2.4.2 – Описание параметров запроса пользователя для завершения идентификации

Параметры	Описание
http(s)://url/redirect	Обратная ссылка на страницу web-сервера прикладной системы (**redirect_uri**)
code	Код авторизации
state	Значение, отправленное в запросе на шаге 3

8) обработку сервером прикладной системы запроса на завершение идентификации пользователя, включающего:

8.1) отправку сервером прикладной системы запроса сервера идентификации на получение маркера доступа по коду завершения идентификации (**code**) методом GET или POST протокола HTTPS вида:

GET/POST

https://id.gov.ua/get-access-token?grant_type=authorization_code&
client_id= client_id &
client_secret= client_secret &
code=code

Примечание.Код авторизации (**code**) может быть использован только один раз.

8.2) обработку запроса и отправку сервером идентификации сервера прикладной системы ответа с маркером доступа в виде JSON-текста вида:

```
Content-Type: application/json {

    «access_token»:«»,
    "token_type":"bearer",
    "expires_in":"",
    "refresh_token":"",
    «user_id»:«»
}
```

Параметры ответа описаны в табл. 2.4.3.

Таблица 2.4.3 – Описание параметров ответа сервера прикладной системы с маркером доступа

Параметры	Описание
access_token	Маркер доступа (значение маркера приведено в качестве примера)
token_type	Тип маркера доступа (имеет фиксированное значение для применения средствами идентификации –**bearer**– доступ по маркеру для предъявителя)
expires_in	Время завершения действия маркера доступа
user_id	Идентификатор идентифицированного пользователя, по которому может быть получена информация о пользователе
refresh_token	Маркер для получения нового маркера доступа

Примечание.Маркер доступа (**access_token**) может быть использован только один раз. Для повторного обращения следует использовать**refresh_token**.

В сервере идентификации идентификаторы идентифицированных пользователей (**user_id**) хранятся вместе с информацией из сертификатов пользователей во временной базе данных (БД) и время завершения действия маркера доступа (**expires_in**) указывает на срок существования соответствующих записей в БД. В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.4.4.

Таблица 2.4.4 – Описание параметров ошибки ответа серверу прикладной системы с маркером доступа

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

8.3) отправку сервером прикладной системы следующего запроса к серверу идентификации на получение информации о пользователе по маркеру доступа (**access_token**) методом GET или POST протокола HTTPS вида:

```
GET/POST

https://id.gov.ua/get-user-info?&access_token=access_token&
    user_id=36&
    fields=firstName,lastName,gender,birthDay,givenname,rnokpp,email,phoneNumber& cert=
```

Параметры запроса описаны в табл. 2.4.5.

Таблица 2.4.5 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
access_token	Маркер доступа
user_id	Идентификатор идентифицированного пользователя (приведенное значение для примера)
fields	Названия полей сертификата запрашиваемых пользователей. Если названия полей (**fields**) не указаны, то возвращаются все доступные поля сертификата с информацией о пользователе (владельце сертификата) и издателе (Предоставитель)

cert	Сертификат шифрования (протокола распределения ключей), на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными поставщиками доверительных услуг, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.

8.4)обработка сервером идентификации запроса путем формирования зашифрованного (с использованием библиотеки подписи в виде модуля расширения PHP и сетевого криптомодуля) ответа с информацией об идентифицированном пользователе в виде JSON-текста вида:

```
Content-Type: application/json {

    "auth_type": "diia_oauth",
    "firstName": "",
    "lastName":"",
    "gender":"",
    "birthDay":"",
    "givenname":"",
    "rnokpp":"",
    «email»:«»,
    "phoneNumber":""
}
```

Все возможные поля пользовательских данных, которые возвращает сервер идентификации после идентификации пользователя (клиента) системы через Действие.OAuth приведены в табл. 2.4.6.

Таблица 2.4.6 - Все возможные поля, возвращаемые сервером идентификации после идентификации пользователя (клиента) системы через Действие OAuth.

Название поля (одно из значений названий полей **fields**)	Описание содержимого поля
firstName	Имя пользователя и отчество пользователя
lastName	Фамилия пользователя
gender	Пол
birthDay	Дата рождения пользователя
givenname	Имя пользователя
rnokpp	РНОКПП пользователя или серия (при наличии) и номер паспорта (для пользователей, которые по своим религиозным убеждениям отказываются от принятия регистрационного номера учетной карточки налогоплательщика и официально сообщили об этом соответствующий контролирующий орган и имеют отметку в паспорте) (Приложение А, п. 8)
email	Электронный адрес пользователя
phoneNumber	Телефон пользователя

Параметры ответа описаны в табл. 2.4.7.

Таблица 2.4.7 – Описание параметров ответа с информацией об идентифицированном пользователе

Параметры	Описание
auth_type	Тип аутентификации, выбранный пользователем (возможные варианты: **diia_oauth**)
firstName, **lastName** и др.	Соответствующие пользовательские данные (значения полей приведены для примера)

Ответ отправляется в виде JSON-текста вида:

```
Content-Type: application/json {

    "encryptedUserInfo":""
}
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"invalid_grant",
    "error_description":""
}
```

Параметры ответа описаны в табл. 2.4.8.

Таблица 2.4.8 – Описание параметров ошибки ответа с информацией об идентифицированном пользователе

Параметры	Описание
error	Тип ошибки (приведенное значение для примера)
error_description	Описание ошибки (приведенное значение для примера)

8.5) отправку сервером идентификации сервера прикладной системы зашифрованного ответа из информацией об идентифицированном пользователе;

8.6) получение и расшифрование сервером прикладной системы ответа с информацией о пользователе (клиенте) и принятие решения сервером прикладной системы о завершении идентификации;

9) отправку сервером прикладной системы ответа пользователю о завершении идентификации.

3 ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ОТДЕЛЬНЫХ ЗАПРОСОВ

3.1 Запрос на продление действия маркера доступа

Запрос состоит из следующих шагов:

1. отправку сервером прикладной системы запроса серверу идентификации на удлинение действия маркера доступа по маркеру удлинение действия маркера доступа (**refresh_token**) методом GET или POST протокола HTTPS вида:

```
GET/POST

https://id.gov.ua/get-refresh-token?grant_type=refresh_token
    &client_id=
    &client_secret=
    &refresh_token=
```

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа с маркером доступа в виде JSON-текста вида:

```
Content-Type: application/json {


    «access_token»:«»,
    "token_type":"bearer",
    «expires_in»:«»
}
```

Настройки ответа описаны в табл.3.1.

Таблица 3.1 – Описание параметров ответа сервера прикладной системы с маркером доступа

Параметры	Описание
access_token	Маркер доступа (значение маркера приведено в качестве примера)
token_type	Тип маркера доступа (имеет фиксированное значение для применения средствами идентификации –**bearer**– доступ по маркеру для предъявителя)
expires_in	Время завершения действия маркера доступа

Примечание.Маркер доступа (**access_token**) может быть использован только один раз. Для повторного обращения следует использовать**refresh_token**.

В сервере идентификации идентификаторы идентифицированных пользователей (**user_id**) сохраняются вместе с информацией из сертификатов пользователей во временной базе данных (БД) и время завершения действия маркера доступа (**expires_in**) указывает на срок существования соответствующих записей в БД. В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {


    "error":"invalid_grant",
    "error_description":""
}
```

3.2 Запрос на удаление данных сессии пользователя

Запрос состоит из следующих шагов:

1. отправка сервером прикладной системы запроса сервера идентификации на удаление данных сессии пользователя по маркеру доступа (access_token) методом GET или POST протокола HTTPS вида:

GET/POST

https://id.gov.ua/get-user-logout?access_token=&user_id=

Параметры запроса описаны в табл. 3.2.

Таблица 3.2 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
access_token	Маркер доступа
user_id	Идентификатор идентифицированного пользователя

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа с маркером доступа в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"0",
    «error_description»:«Данные пользователя с ID = user_id удалены успешно»
}
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json {

    "error":"1",
    «error_description»:«»
}
```

3.3 Запрос на проверку данных пользователя по Государственному реестру физических лиц – налогоплательщиков (ГРФЛ)

Для проверки данных пользователя необходимо запросить проверку**get-user-drfo-check-request**

Запрос состоит из следующих шагов:

1. отправка сервером прикладной системы запроса сервера идентификации на проверку данных пользователя по реестру физических лиц по маркеру доступа (access_token) методом POST протокола HTTPS вида:

POST

https://id.gov.ua/get-user-drfo-check-request

Предоставление данных происходит на основании маркера доступа (**access_token**), полученного в ходе авторизации. Маркер доступа передается в заголовке запроса (**headers**) в виде:

Authorization:**access_token значение_маркера_доступа**

Таблица 3.3.1 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
cert	Сертификат протокола распределения ключей, на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными предоставляющими доверительные услуги, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.
user_id	Идентификатор идентифицированного пользователя

При запросе в реестр предоставляются данные пользователя, которые возвращаются по запросу**get-user-info.**

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа (возможные значения ответа приведены в таблице 3.3.3 Значения приводятся как они есть в документации к соответствующему сервису ДРФЛ) в виде JSON-текста вида:

```
Content-Type: application/json
{
    «encryptedResponse»:«Защищенное (зашифрованное) содержимое ответа от сервиса ДРФЛ»
}
```

Ответ от сервиса передается как есть в полном объеме. Зашифрование осуществляется на сертификате клиента, который передается при запросе в параметре**cert**.

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json
{
    «error»:«номер ошибки»,
    «error_description»:«описание ошибки»
}
```

Структура ответа от сервиса ГРФЛ приведена в табл. 3.3.2

Таблица 3.3.2 – Структура ответа сервиса ГРФЛ

№	Название	Уровень вложенности	Описание реквизита	Тип данных	Обязанность ковость значения поля	Примечание
1	Result	1-й уровень	Результат обработки	xs:string	O	Принимает значение в соответствии с справочника результатов обработки
2	Errormsg	1-й уровень	Сообщение об ошибках	xs:string		если поле RESULT=0, ERRORMSG – не заполняется; если поле RESULT не равно 0, поле ERRORMSG заполняется данными, которые отправлено в запросе (application number (уникальный идентификатор запроса в ГНС), executoredrpou, executorrnokpp; executorfullname; rnokpp;last_name; first_name; middle_name; date_birth)

Таблица 3.3.3 – Описание значений пользовательского статуса

Значение	Описание
0	регистрационный номер учетной карточки налогоплательщика/серия (при наличии) и номер паспорта и реквизиты «Фамилия», «Имя» и «Отчество» (при наличии), указанные в запросе, соответствуют информации, имеющейся в Государственном реестре;
1	недействующий регистрационный номер учетной карточки налогоплательщика/ физическое лицо с указанными в запросе серией (при наличии) и номером паспорта на учете не состоит
2	регистрационный номер учетной карточки налогоплательщика закрыт/физическое лицо с указанными в запросе серией (при наличии) и номером паспорта снят с учета
3	в запросе не заполнены или некорректно заполнены поля, обязательные для заполнения
4	реквизит «регистрационный номер учетной карточки налогоплательщика/серия (при наличии) и номер паспорта» и реквизиты «Фамилия», «Имя» и «Отчество» (при наличии), указанные в запросе, не соответствуют имеющейся информации в Государственном реестре
42	реквизит «регистрационный номер учетной карточки налогоплательщика/ серия (при наличии) и номер паспорта» и реквизиты «Фамилия», «Имя» и «Отчество» (при наличии), указанные в запросе, не соответствуют имеющейся информации в Государственном реестре, и регистрационный номер учетной карточки налогоплательщика закрыт/ физическое лицо с указанными в запросе серией (при наличии) и номером паспорта снят с учета

3.4 Запрос на проверку документов пользователя по реестру утраченных документов единой информационной системы МВД (ЕИС МВД)

Для проверки данных пользователя необходимо запросить проверку**get-user-documentloss-check**

Запрос состоит из следующих шагов:

1. отправку сервером прикладной системы запроса серверу идентификации на проверку пользовательских данных по реестру физических лиц по маркеру доступа (**access_token**) методом POST протокола HTTPS вида (описание параметров в табл. 3.4.1):

POST

https://id.gov.ua/ get-user-documentloss-check

Предоставление данных происходит на основании маркера доступа (**access_token**), полученного в ходе авторизации. Маркер доступа передается в заголовке запроса (**headers**) в виде:

Authorization:**access_token значение_маркера_доступа**

Таблица 3.4.1 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
cert	Сертификат протокола распределения ключей, на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными предоставляющими доверительные услуги, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.
user_id	Идентификатор идентифицированного пользователя

При запросе в реестр предоставляются данные пользователя, которые возвращаются по запросу**get-user-info.**

Проверка производится по номеру паспорта. Номер паспорта для проверки получается с поля РНОКПП (если пользователь отказывался от получения персонального налогового номера) или с ручного ввода пользователя при подтверждении согласия на передачу данных.

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа (возможные значения ответа приведены в таблицах 3.4.2 Значения приводятся как они есть в документации к соответствующему сервису ЕИС МВД) в виде JSON-текста вида:

```
Content-Type: application/json
{
    «encryptedResponse»:«Защищенное (зашифрованное) содержимое ответа от сервиса ЕИС МВД»
}
```

Ответ от сервиса передается как есть в полном объеме. Зашифрование осуществляется на сертификате клиента, хранящемся в БД (реестре подключенных клиентов).

Пример ответа, в виде JSON-текста вида:

```
(
[DOC_VID_TEXT] => ПАСПОРТ ГРАЖДАНИНА УКРАИНЫ
[DOC_SER] => AB
[DOC_NOM] => 000011
[DOC_VYDAN] => 1995-07-13T03:00:00.000+03:00
[ORGAN_COD] => 111111
[ORGAN_TEXT] => РАЙОННОЕ ОТДЕЛЕНИЕ ПОЛИЦИИ
[DATE_INPUT] => 2002-12-12T02:00:00.000+02:00
[DATE_APPEALL] => 2002-12-02T02:00:00 => УТРАЧЕНО

)
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

```
Content-Type: application/json
{
    «error»:«номер ошибки»,
    «error_description»:«описание ошибки»
}
```

Таблица 3.4.2 – Описание параметров ответа ЕИС МВД

Параметры	**Тип данных**	**Обязательный (R) / Опциональный (O)**	**Описание**
DOC_VID_TEXT	string	R	Вид документа (текст)
DOC_SER	string	O	Серия документа
DOC_NOM	string	O	Номер документа
DOC_VYDAN	date	R	Дата выдачи документа
ORGAN_COD	numeric	R	Орган предоставления информации (код)
ORGAN_TEXT	string	R	Орган предоставления информации (текст)
DATE_INPUT	date	R	Дата постановки на учет органом
DATE_APPEALL	date	R	Дата обращения в орган
PRI_TEXT	string	R	Причина учета (текст)

3.5 Запрос на получение данных по коду РНОКПП (физического лица – предпринимателя) по Единому государственному реестру юридических лиц, физических лиц-предпринимателей и общественных формирований (ЕГР)

Для проверки данных пользователя необходимо запросить проверку**get-user-edr-drfo**

Запрос состоит из следующих шагов:

1. отправку сервером прикладной системы запроса серверу идентификации на проверку пользовательских данных по реестру физических лиц по маркеру доступа (**access_token**) методом POST протокола HTTPS вида (описание параметров в табл. 3.5.1):

POST

https://id.gov.ua/get-user-edr-drfo

Предоставление данных происходит на основании маркера доступа (**access_token**), полученного в ходе авторизации. Маркер доступа передается в заголовке запроса (**headers**) в виде:

Authorization:**access_token значение_маркера_доступа**

Таблица 3.5.1 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
cert	Сертификат протокола распределения ключей, на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными предоставляющими доверительные услуги, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.
user_id	Идентификатор идентифицированного пользователя

При запросе в реестр предоставляются данные пользователя, которые возвращаются по запросу**get-user-info.**

Проверка (запрос в ЭДР) осуществляется по коду ДРФЛ или по той информации (номер/серия паспорта), которая указана в данных кода ДРФЛ пользователя.

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа (возможные значения ответа приведены в таблице 3.5.2. Значения приводятся как они есть в документации к соответствующему сервису ЕГР) в виде JSON-текста вида

Content-Type: application/json

{

«encryptedResponse»:«Защищенное (зашифрованное) содержимое ответа от сервиса ЕГР»

}

Ответ от сервиса передается в соответствии с приведенным набором данных. Зашифрование осуществляется на сертификате клиента, который передается при запросе в параметре**cert**.

Пример ответа если у пользователя указан ДРФЛ, в виде JSON-текста вида:

```
[Subject] => (
        [state_text] => прекращено
        [code] => 1234554321
        [passport] =>
        [birthday] =>
        [names] => (
                [name] => ТЕСТОВЫЙ ПОЛЬЗОВАТЕЛЬ ПЕТРОВИЧ
        )
        [address] => (
                [zip] => 61001
                [country] => Украина
                   [address] => Украина, 61001, Харьковская обл., город Харьков, УЛИЦА СУМСКАЯ, дом 1, квартира 1
                [parts] => (
                        [atu] => Харьковская обл., город
                        Харьков [street] => УЛИЦА СУМСКАЯ
                        [house_type] => дом
                        [house] => 1
                        [num_type] => квартира
                        [num] => 1
                        [atu_code] => 1234567890
                )
        )
        [registration] => (
                [date] => 2015-01-01
                [record_date] => 2015-01-01
        )
)
```

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

Content-Type: application/json

{
«error»:«номер ошибки**»,**
«error_description»:«описание ошибки**»**
}

Таблица 3.5.2 – Описание параметров ответа в ЕГР

Параметры	**Уровень вложенности**	**Описание**
Subject	1	Контейнер для информации о субъекте
state_text	2	Текстовое отображение состояния субъекта
code	2	Код по ЕГРПОУ или РНОКПП
passport	2	Серия и/или номер документа ФЛП
birthday	2	Дата рождения ФЛП
names	2	Список наименований субъекта
name	3	Название юридического лица
address	2	Адрес
zip	3	Почтовый индекс
country	3	Название страны
address	3	Адрес
parts	3	Адрес в развернутом виде
atu	4	Административная территориальная единица
street	4	Улица
house_type	4	Тип здания
house	4	Номер здания
num_type	4	Тип помещения
Num	4	Номер помещения
atu_code	4	Код административно-территориальной единицы (КОАТУУ)
registration	2	Сведения о регистрации
date	3	Дата регистрации
record_date	3	Номер записи о регистрации

3.6 Запрос на получение данных и проверки соответствия РНОКПП пользователя к юридическому лицу по ЕГРПОУ за ЕГР

Для проверки данных пользователя необходимо запросить проверку**get-user-edr-edrpou**

Запрос состоит из следующих шагов:

1. отправку сервером прикладной системы запроса серверу идентификации на проверку пользовательских данных по реестру физических лиц по маркеру доступа (**access_token**) методом GET или POST протокола HTTPS вида (описание параметров в табл. 3.6.1):

POST

https://id.gov.ua/get-user-edr-edrpou

Предоставление данных происходит на основании маркера доступа (**access_token**), полученного в ходе авторизации. Маркер доступа передается в заголовке запроса (**headers**) в виде:

Authorization:**access_token значение_маркера_доступа**

Таблица 3.6.1 – Описание параметров запроса на получение информации о пользователе сервером прикладной системы

Параметры	Описание
cert	Сертификат протокола распределения ключей, на который будет зашифрован ответ сервером идентификации, в формате BASE64. **Примечание**. Сертификат шифрования выдается квалифицированными предоставляющими доверительные услуги, перечень которых доступен на вебсайте ЦЗО https://www.czo.gov.ua/ca-registry. Код ЕГРПОУ, указанный в сертификате шифрования, должен соответствовать коду ЕГРПОУ юридического лица, с которым заключен договор о присоединении к ИСЕИ.
user_id	Идентификатор идентифицированного пользователя

При запросе в реестр предоставляются данные пользователя, которые возвращаются по запросу**get-user-info.**

Если во время идентификации, данные пользователя не содержат код ЭДРПОУ, такое поле будет предложено пользователю для ручного ввода при подтверждении передачи данных.

Если пользовательские данные содержат и поле ДРФО и поле ЕГРПОУ выполняется поиск и сравнение по коду РНОКПП в данных организации (юридического лица) среди руководителей и подписантов.

Если данные РНОКПП отсутствуют, а указаны только данные ЕГРПОУ, предоставляется полная информация о руководителях и подписантах организации (юридического лица) по указанному ЕГРПОУ, за исключение РНОКПП руководителей и подписантов организации (юридического лица).

2. обработку запроса и отправку сервером идентификации сервера прикладной системы ответа (возможные значения ответа приведены в таблице 3.6.2. Значения приводятся как они есть в документации к соответствующему сервису ЕГР) в виде JSON-текста вида

```
Content-Type: application/json
{
    «encryptedResponse»:«Защищенное (зашифрованное) содержимое ответа от сервиса ЕГР»
}
```

Ответ от сервиса передается в соответствии с приведенным набором данных. Зашифрование осуществляется на сертификате клиента, который передается при запросе в параметре**cert**.

Пример ответа если у пользователя указан РНОКПП и он отвечал некоторым должностям по указанному ЕГРПОУ, в виде JSON-текста вида:

```
[Subject] => Array (
        [code] => 11223344
        [names] => Array (
                [name] => "ТЕСТ1"
                [include_olf] => 1
                [display] => ЧАСТНОЕ ПРЕДПРИЯТИЕ "ТЕСТ1" [short]
                => ЧП "ТЕСТ1"
        )
        [address] => Array (
                [zip] => 11001
                [country] => Украина
                [address] => Украина, 11001, город Киев, УЛИЦА СТЕПОВАЯ, дом 1
                [parts] => Array (
```

[atu] => город Киев [street] =>
УЛИЦА СТЕПНАЯ [house_type]
=> дом
[house] => 1
[atu_code] => 1234567890
)
)
[registrations] => Array (
[0] => Array (
[reg_number] =>
[start_date] =>
[start_num] =>
[end_date] =>
[end_num] =>
)
)
[heads] => Array (
[0] => Array (
[rnokpp] => 1234554321
[birthday] =>
[last_name] => ТЕСТОВЫЙ [first_middle_name] =>
ПОЛЬЗОВАТЕЛЬ ПЕТРОВИЧ [role] => 3
[role_text] => руководитель
[position] =>
[appointment_date] => 2011-03-09
[restriction] => СОГЛАСНО УСТАЛУ
)
[1] => Array (
[rnokpp] => 1234554321
[birthday] =>
[last_name] => ТЕСТОВЫЙ [first_middle_name] =>
ПОЛЬЗОВАТЕЛЬ ПЕТРОВИЧ [role] => 2
[role_text] => подписант
[position] =>
[appointment_date] => 2011-03-09
[restriction] => Совершать действия от имени юридического лица, в том числе подписывать договоры и т.п. (согласно Уставу)
)
)
)

В случае ошибки обработки запроса отправляется структура в виде JSON-текста вида:

Content-Type: application/json

{
«error»:«номер ошибки**»,**
«error_description»:«описание ошибки**»**
}

Таблица 3.6.2 – Описание параметров ответа по ЕГР

Параметры	**Уровень вложенности**	**Описание**
Subject	1	Контейнер для информации о субъекте
code	2	Код по ЕГРПОУ или РНОКПП
names	2	Список наименований субъекта
name	3	Название юридического лица
address	2	Адрес
zip	3	Почтовый индекс
country	3	Название страны
address	3	Адрес
parts	3	Адрес в развернутом виде
atu	4	Административная территориальная единица
street	4	Улица
house_type	4	Тип здания
house	4	Номер здания
num_type	4	Тип помещения
num	4	Номер помещения
atu_code	4	Код административно-территориальной единицы (КОАТУУ)
registrations	2	Сведения, полученные в порядке взаимодействия с информационными системами органов государственной власти
reg_number	3	Номер регистрации
start_date	3	Дата взятия на учет
start_num	3	Номер взятия на учет
end_date	3	Дата снятия с учета
end_num	3	Номер снятия с учета
heads	2	Фамилия, имя, отчество, должность, дата избрания (назначения) лиц, избираемых (назначаемых) в орган управления юридического лица, уполномоченных представлять юридическое лицо в правоотношениях с третьими лицами, или лиц, имеющих право совершать действия от имени юридического лица без доверенности, в том числе подписывать договоры и данные о наличии ограничений по представительству от имени юридического лица
head	3	Сведения о личности
rnokpp	4	РНОКПП
birthday	4	Дата рождения

last_name	4	Назначенное уполномоченное лицо
first_middle_name	4	Фамилия
role	4	Имя и отчество
role_text	4	Роль по отношению к связанному субъекту
position	4	Текстовое отображение роли
appointment_date	4	Должность
restriction	4	Дата назначения
branches	2	Перечень обособленных подразделений юридического лица
branch	3	Обособленное подразделение юридического лица
name	4	Наименование обособленного подразделения
code	4	Код по ЕГРПОУ обособленного подразделения
role_text	4	Роль по отношению к связанному субъекту (текстовое отображение)
type_text	4	Тип обособленного подразделения (текстовое отображение)
create_date	4	Дата записи о создании обособленного подразделения
address	4	Адрес обособленного подразделения
		+ Все поля по аналогии с адресом субъекта
heads	4	Сведения о руководителе обособленного подразделения: фамилия, имя, отчество, должность, дата назначения, наличие ограничений по представительству от имени юридического лица
head	5	Назначенное уполномоченное лицо
last_name	6	Фамилия
first_middle_name	6	Имя и отчество
role	6	Роль по отношению к связанному субъекту
role_text	6	Текстовое отображение роли
position	6	Должность
appointment_date	6	Дата назначения
restriction	6	Ограничение

4 ПОРЯДОК ПОДКЛЮЧЕНИЯ СЕРВИСА СОЗДАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ (ОТЖЕТА ПОДПИСИ)

Подключение сервиса создания и проверки электронной подписи (виджета подписи) производится для возможности наложения/проверки электронной подписи на файлах пользователей через веб.

Для подключения виджета к странице web-сайта необходимо:

1) подключить скрипт взаимодействия eusign.js к странице:

```
<script type="text/javascript" src="eusign.js"></script>
```

2) создать батковский элемент на странице в котором будет отображаться iframe:

```
<div id="sign-widget-parent"  style="width:700px;height:500px">
```

3) создать объект для взаимодействия с iframe:

```
var euSign = new EndUser(
    "sign-widget-parent",  /* Идентификатор батковского элемента */ /*
    "sign-widget",  Идентификатор элемента iframe */
    "https://id.gov.ua/sign-widget/v20220527/",
                            /* URI для загрузки iframe */ /* Тип формы
    EndUser.FormType.SignFile  iframe */
) ;
```

Подробное описание методов и параметров находится в java-скрипт-файле eusign.js.

URI для загрузки iframe сервиса наложения и проверки подписи:

1. Наложение подписи

   https://id.gov.ua/sign-widget/v20220527/

2. Проверки подписи

   https://id.gov.ua/verify-widget/v20220527/

При необходимости создать отдельные файлы для изменения внешнего вида [DNS-имя web-сайта].css виджета.

Примечание.Файлы стилей прилагаются по обращению в адресcontract@id.gov.ua

ПРИЛОЖЕНИЕ А. ПРАВИЛА ПРОВЕРКИ ВХОДНЫХ ПАРАМЕТРОВ

Регулярные выражения для проверки входных параметров:

1) Регулярное выражение проверки параметра**client_id:**

/^[0-9A-Za-z]+$/

2) Регулярное выражение проверки параметра**client_secret:**

/^[0-9ABCDEFabcdef]+$/

3) Регулярное выражение проверки параметра**code**(код авторизации):

/^[0-9ABCDEFabcdef]+$/

4) Регулярное выражение проверки параметра**access_token (маркера доступа):**

/^[0-9ABCDEFabcdef]+$/

5) Регулярное выражение проверки параметра**auth_type:**

/^[az_\,]+$/

6) Регулярное выражение проверки параметра**state:**

/^[0-9A-Za-z_\-\=]{10,512}+$/

7) Регулярное выражение проверки параметра**redirect_uri:**

/\b(?:(?:https?|http):\/\/|www\.)[-a-z0-9+&@#\/%?=~_|!:,.;]* [-a-z0-9+&@#\/%=~_|]/i

8) Регулярное выражение проверки параметра**drfocode:**

([0-9]{10}|[АБВГДЕЕЖЗИИКЛМНОПРСТУФХЦЧШЩЮЯ]{2}[0-9]{6}|[0-9]{9})

ПРИЛОЖЕНИЕ Б. ОШИБКИ ПРИ ИСПОЛЬЗОВАНИИ СЕРВИСОВ ИСЕИ

1) Ошибка проверки кода авторизации (Ошибка: 1)**:**

Переданный параметр client_id не соответствует регулярному выражению. Регулярные выражения для проверки входных параметров указаны в Приложении А.

2) Ошибка проверки кода авторизации (Ошибка: 2)**:**

Переданный параметр client_secret не соответствует регулярному выражению. Регулярные выражения для проверки входных параметров указаны в Приложении А.

3) Ошибка проверки кода авторизации (Ошибка: 3):

Переданный параметр code не соответствует регулярному выражению. Регулярные выражения для проверки входных параметров указаны в Приложении А.

4) Ошибка проверки кода авторизации (Ошибка: 4)**:**

Просроченный токен (токен активен 30 секунд)
OAUTH_CODES_EXPIRED_SECONDS = 30;

5) Ошибка проверки кода авторизации (Ошибка: 9)**:**

Попытка повторно использовать код авторизации. Код должен использоваться один раз.

6) Ошибка проверки кода авторизации (Ошибка: 10)**:**

Использован неправильный параметр client_id или client_secret.

7) Возникла ошибка при считывании личных ключей. Возникла ошибка при считывании личного ключа с носителя ключевой информации (18)**:**

Неверно введен пароль к ключу (ключ на защищенном носителе ключевой информации).

8) Возникла ошибка при считывании личных ключей. Возникла ошибка при считывании личного ключа с носителя ключевой информации (19)**:**

Выбран неправильный тип носителя или на носителе нет личного ключа. Необходимо выбирать тип носителя без сообщения "носитель".

9) Возникла ошибка при открытии личного ключа (неверный пароль или ключ поврежден)(24)**:**

Неверно введен пароль к ключу (файловый ключ).

10) Сертификат поврежден или не может быть использован (50)

Невозможно проверить статус сертификата или сертификат недействителен.

11) Ошибка при разборе ответа от TSP-сервера(66)

Невозможно проверить статус сертификата.

12) Возникла ошибка при идентификации. Код ошибки: 112. Описание ошибки: Использование тестовых сертификатов запрещено

При авторизации использованы тестовые сертификаты. Использование тестовых сертификатов разрешено только на тестовой среде ИСЭИ.

13) Ошибка при получении данных клиента (400)

Ошибка встречается при авторизации с помощью BankID. Ошибка означает, что данные клиента внесены не верно или не полностью. Для решения ошибки клиенту необходимо обратиться в банковское учреждение для проверки внесенных данных.

14) Код ЕГРПОУ в сертификате шифрования не соответствует коду ЕГРПОУ юридического лица, заключающего договор с ГП "ДЕЯ"

При направленном шифровании код ЕГРПОУ в сертификате шифрования не соответствует коду ЕГРПОУ юридического лица, заключающего договор с ГП "ДЕЯ"

15) Возникла ошибка при идентификации. Код ошибки: 900. Описание ошибки: Возникла ошибка проверки РНОКПП

У авторизуемого пользователя не заполнен РНОКПП/серия и/или номер паспорта. Пользователю необходимо обратиться к поставщику электронных доверительных услуг/Банковского учреждения.

16) Обратите внимание! Запросы авторизации от системы не отвечают требованиям RFC 6749 к параметру state, что может нести риски для пользователя.
Рекомендуем обратиться к владельцу системы

Переданный параметр state не соответствует регулярному выражению. Регулярные выражения для проверки входных параметров указаны в Приложении А.

17) Обратите внимание! Вы перешли по прямой ссылке. Вы можете только проверить возможность идентификации

Авторизоваться нужно на вебсайте информационной системы, из которой осуществляется переход на вебсайт ИСЕИ (id.gov.ua). Проблема может возникнуть, если пользователь открывает ссылку в новой вкладке или переходит на предыдущую страницу после нажатия авторизоваться.

18) Поле redirect_uri не соответствует Системе, с которой Вы выполняете подключение. Переход по указанной ссылке может быть опасен

Для использования ресурсов ИСЕИ информационная система получает маркеры доступа на конкретное имя домена и соответствующий ему redirect_uri.
Redirect_uri – это обратная ссылка на web-сервер прикладной системы, на которую сервер идентификации (id.gov.ua) перенаправляет браузер пользователя после осуществления им авторизации. Если в информационной системе изменился redirect_uri, необходимо обратиться к техническому администратору ИСЕИ для внесения соответствующих изменений.

ПРИЛОЖЕНИЕ В. ССЫЛКИ НА БИБЛИОТЕКИ ПОДПИСЬ ПОЛЬЗОВАТЕЛЯ ЦСК И ПРИМЕРЫ ИХ ИСПОЛЬЗОВАНИЕ

Примеры использования системы эл. идентификации (ИСЕИ) в Действие (Минцифри):

1) с использованием Java-библиотеки

2) с использованием JavaScript-библиотеки (для среды выполнения NodeJS)

3) с использованием Python-библиотеки

4) с использованием C#-библиотеки (со считыванием ключей также и с аппаратных носителей)

5) с использованием библиотеки с интерфейсом C++

6) с использованием PHP-библиотеки подписи пользователя ЦСК

https://iit.com.ua/download/EUSignCP-EID-Usages-20241218.zip

Примеры подключения веб-виджета (iframe) на веб-страницу в ИСЕИ:

https://id.gov.ua/downloads/EUSignWidget(Usage)-20220527.zip

Актуальные библиотеки пользователя ЦСК (из состава программного комплекса (ПК) пользователя ЦСК "IIT Пользователь ЦСК-1"):

1) Java-библиотека подписи пользователя ЦСК – https://

iit.com.ua/download/EUSignCP-Java-20241115.zip

2) JavaScript-библиотека подписи пользователя ЦСК (для среды выполнения NodeJS в т.ч.) – https://

iit.com.ua/download/EUSignCP-JS-20241025.zip

3.1) Библиотека подписи пользователя ЦСК с Python-интерфейсом для ОС Linux –

https://iit.com.ua/download/EUSignCP-Linux-Python-20241126.zip

3.2) Библиотека подписи пользователя ЦСК с Python-интерфейсом для ОС Microsoft Windows -

https://iit.com.ua/download/EUSignCP-MSWindows-Python-20241125.zip

4.1) Библиотека подписи пользователя ЦСК для ОС Microsoft Windows с C#-интерфейсом

https://iit.com.ua/download/EUSignCP-CS-NuGet-20241204.zip

4.2) Библиотека подписи пользователя ЦСК для среды выполнения (фреймворка) .NET Core из C#-интерфейсом для ОС Microsoft Windows, Linux и Apple macOS -

https://iit.com.ua/download/EUSignCP-CS-NetCore-20240626.zip

5.1) Библиотека подписи пользователя ЦСК с C/C++-интерфейсом для ОС Linux для архитектур Intel X86 32/64 https://iit.com.ua/download/EUSignCP-Linux-20250102.zip

5.2) Библиотека подписи пользователя ЦСК с C/C++-интерфейсом для ОС Microsoft Windows архитектур Intel X86 32/64 - https://iit.com.ua/download/EUSignCP-MSWindows-20241114.zip

6) PHP-библиотека подписи пользователя ЦСК – https://iit.com.ua/download/EUSPHPE-20241230.zip

Актуальный список сертификатов совместимых поставщиков -

https://iit.com.ua/download/productfiles/CACertificates.p7b Актуальные

параметры взаимодействия с совместимыми поставщиками - https://

iit.com.ua/download/productfiles/CAs.json

ВЕРСИИ

ДАТА УТВЕРЖДЕНИЯ	ВЕРСИЯ ДОКУМЕНТА
06.01.2025	V15_06012025
31.07.2024	V14_31072024
18.06.2024	V13_18062024
11.10.2023	V12_11102023
15.03.2023	V11_15032023
12.01.2023	V10_12012023
25.04.2022	V9_25042022
23.11.2021	V8_23112021
17.11.2021	V7_17112021
24.05.2021	V6_24052021
20.05.2021	V5_20052021
11.05.2021	V4_11052021
16.03.2021	V3_16032021
10.03.2021	V2_10032021
11.01.2021	V1_11012021